

A non-distillability criterion for secret correlations

Lluís Masanes¹, Andreas Winter^{2,3}

¹*ICFO-Institut de Ciències Fotoniques, 08860 Castelldefels (Barcelona), Spain*

²*Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.*

³*Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Within entanglement theory there are criteria which certify that some quantum states cannot be distilled into pure entanglement. An example is the positive partial transposition criterion. Here we present, for the first time, the analogous thing for secret correlations. We introduce a computable criterion which certifies that a probability distribution between two honest parties and an eavesdropper cannot be (asymptotically) distilled into a secret key. The existence of non-distillable correlations with positive secrecy cost, also known as bound information, is an open question. This criterion may be the key for finding bound information. However, if it turns out that this criterion does not detect bound information, then, a very interesting consequence follows: any distribution with positive secrecy cost can increase the secrecy content of another distribution. In other words, all correlations with positive secrecy cost constitute a useful resource.

I. INTRODUCTION

Information theoretic cryptology started with Shannon [20], and it established that secret communication relied entirely on secret key; but not until Wyner's famous wiretap paper [23] was it recognized that noise in the eavesdropper's channel can be used to establish secrecy in a communication. The secrecy capacity of what is now called the general wiretap channel was determined in [7]. After that, again, it took some while before the distillation of key from given correlation P_{ABE} between two cooperating players, Alice (A) and Bob (B), and an eavesdropper Eve (E) was considered [2, 16], in a model where the three parties share a large number of copies of the given distribution P_{ABE} , and Alice and Bob can freely exchange messages over an authenticated but public channel (i.e., monitored by Eve).

Indeed, Maurer [16] showed that this scenario is much richer than the one of the wiretap channel. His paper posed the problem of determining the optimal secret key rate of any given distribution P_{ABE} , in the discrete memoryless setting of availability of asymptotically many independent samples of the distribution, and in particular the problem of deciding whether a distribution can be distilled into a secret key or not.

There has by now been a long history of fruitful exchange of ideas between cryptography and entanglement theory (see e.g. [3]), mostly relating protocols for secret key and entanglement distillation. In the quantum case, the reverse process was considered in [3]: create a quantum state from pure entanglement with maximum efficiency. Subsequently it was shown that there exist states that require a positive rate of entanglement to be created, but yield no pure entanglement at all under any distillation procedure. These states are called *bound entanglement* [9, 21]. The key to show the existence of bound entanglement is the positive partial transposition criterion [18], which certifies that a given state is not distillable.

This motivated Gisin and Wolf [8] to speculate on the existence of *bound information*, i.e. distributions that yield no secret key under distillation but nevertheless somehow contain secrecy. They presented some candidates for bound information derived from bound entangled quantum states. Subsequently, the notion of secret key cost of a given distribution P_{ABE} was formalised (under the name *information of formation*) [19]. Roughly speaking, this is the minimum amount of secret bits that are necessary in order to generate P_{ABE} from public communication. Latter, a single-letter formula for this quantity was found [22].

Renner and Wolf [19] have shown that there can be arbitrarily large gaps between the secret key cost and the key distillation rate, thus providing evidence for the existence of bound information (see also [22]). In [1, 13] it was shown that *multipartite* (i.e., more than two honest players) bound information indeed exists. But nothing is known about the existence of bound information in the bipartite case. The reason is that no criterion for non-distillability of secret correlations is known. In this paper we present the first one, which is based on the idea presented in [14, 15].

II. NOTATION

Key distillation and key cost are most conveniently expressed via the probability distribution from which Alice, Bob and Eve observe samples. A generic multipartite probability distribution among the parties $AB\dots$ is denoted by a non-negative vector $P_{AB\dots}$ belonging to the \mathbb{R} -linear space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \dots$ which comes with a distinguished (tensor product) basis. This distinguished, “computational”, basis of the local space \mathcal{H}_A has one element for each outcome from the alphabet of A . For instance, the computational basis of a bit \mathcal{B} consists of the two vectors $(1, 0)$ and $(0, 1)$. Note that for generic alphabets we use \mathcal{H} to denote the vector space, but for bits (two dimensions) we reserve \mathcal{B} . Furthermore, to

identify which party has access to the sample from a factor in the tensor product, we attach generic indices A , B and E ; if the space of one party consists of several alphabets, we denote them A , A' , A'' , etc. The coefficients of $P_{AB\dots}$ in the computational (product) basis are denoted by $P_{AB\dots}(a, b, \dots)$, and each corresponds to the probability of the event with outcomes (a, b, \dots) . Hence all the coefficients of $P_{AB\dots}$ must be non-negative. Unless explicitly mentioned, we allow probability distributions $P_{AB\dots}$ to be not normalized.

A general (stochastic) operation \mathcal{M} , which may be filtering (i.e., not preserving probability), is represented by a linear map with non-negative coefficients $\mathcal{M} : \mathcal{H}_1 \rightarrow \mathcal{H}_2$. Because we do not care about normalization, there is no additional constraint on the coefficients of \mathcal{M} , apart from non-negativity. In the case of local operations, we specify which party performs each operation by attaching an appropriate index, e.g. $\mathcal{M}_A \mathcal{N}_B$. We omit the tensor product sign, and the identity matrix for the remaining parties.

III. PRELIMINARY RESULTS

The secret bit fraction was introduced in [12], as the secrecy analog of the quantum singlet fraction, introduced in [11].

Definition 1 (secret bit fraction). Suppose P_{ABE} is a tripartite normalized probability distribution, where the outcomes corresponding to parties A and B take values on $\{0, 1\}$. The secret bit fraction of P_{ABE} , denoted $\lambda[P_{ABE}]$, is the maximum value of μ for which a decomposition

$$P_{ABE} = \mu S_{AB} P'_E + (1 - \mu) P''_{ABE} \quad (1)$$

exists, where P'_E and P''_{ABE} are arbitrary normalized distributions, and S is a secret bit shared by two parties: $S(a, b) = \frac{1}{2} \delta_{a,b}$.

Lemma 2. The secret bit fraction of P_{ABE} can be written as

$$\lambda[P_{ABE}] = 2 \frac{\sum_e \min\{P_{ABE}(0, 0, e), P_{ABE}(1, 1, e)\}}{\sum_{a,b,e} P_{ABE}(a, b, e)}. \quad (2)$$

This is proven in [12]. We have included the normalization factor in the denominator of (2) in order not to worry about the normalization of P_{ABE} ; in this way, the quantity $\lambda[P_{ABE}]$ makes sense irrespective of normalization of P_{ABE} . Note that $\lambda[P_{ABE}] = 1$ means that $P_{ABE} = S_{AB} P'_E$, so that P_{ABE} represents a *secret bit* between Alice and Bob.

Definition 3. The maximal extractable secret bit fraction of a given distribution $P_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is

$$\Lambda[P_{ABE}] = \sup_{\mathcal{M}_A, \mathcal{N}_B} \lambda[\mathcal{M}_A \mathcal{N}_B P_{ABE}], \quad (3)$$

where the optimization is made over maps $\mathcal{M}_A : \mathcal{H}_A \rightarrow \mathcal{B}$ and $\mathcal{N}_B : \mathcal{H}_B \rightarrow \mathcal{B}$.

Note that the function $\lambda[P_{ABE}]$ is only defined for distributions P_{ABE} where the alphabets of A, B are $\{0, 1\}$, hence, in the definition of Λ , it is important that the range of the maps $\mathcal{M}_A, \mathcal{M}_B$ is \mathcal{B} . On the other hand, the function Λ is defined on probability distributions P_{ABE} for random variables taking values on arbitrary alphabets. The maximal extractable secret bit fraction expresses the quality of the secret bit that can be extracted from a single copy of a given distribution. If $\Lambda[P_{ABE}] = 1$ then a perfect secret bit can be extracted from a single copy of P_{ABE} . If P_{ABE} is the product of two uniformly random bits (one for each of the honest parties) and any uncorrelated information for Eve, then $\Lambda[P_{ABE}] = 1/2$. Because the output of the maps $\mathcal{M}_A, \mathcal{M}_B$ can always be an independent uniform random bit, irrespectively of the input, the range of Λ is $[1/2, 1]$. It is shown in [12] that the quantity Λ is a secrecy monotone, and hence, constitutes a measure of the amount of secrecy contained in a given P_{ABE} . Additionally, there is a relation between this single-copy secrecy measure and asymptotic distillability. It is shown in [12] that if $\Lambda[P_{ABE}] > 1/2$ then P_{ABE} is distillable. In what follows we rephrase the definition of distillability in terms of Λ .

Definition 4 (Distillability). We say that the distribution $P_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is (secret-key-)distillable if for each $\lambda_0 \in [1/2, 1)$ there exists an integer n such that $\Lambda[P_{ABE}^{\otimes n}] > \lambda_0$.

That is, from a sufficiently large number of copies of P_{ABE} , Alice and Bob can, by local operations and public communication (which, without loss of generality, can be assumed to be a filtering of the form written in (3)), obtain arbitrarily good approximations to a secret bit. If there exists n such that $\Lambda[P_{ABE}^{\otimes n}] > 1/2$, one can apply advantage distillation [16] to the result and obtain a secret key (see [12]). Note furthermore that in this case even positive rates of secret key can be obtained, as $n \rightarrow \infty$. (The reader familiar with entanglement theory will realize the similarity of these concepts to singlet fraction and singlet distillability.) The difficulty in dealing with distillability is that its definition involves an arbitrarily large number of copies of P_{ABE} . The following tools deal with this problem.

Lemma 5. Let $\mathcal{H}_1, \mathcal{H}_2$ and \mathcal{H}_3 be given vector spaces. Any “global” linear map $\mathcal{M} : \mathcal{H}_1 \otimes \mathcal{H}_2 \rightarrow \mathcal{H}_3$ with non-negative coefficients can be decomposed into a local linear map with non-negative coefficients, $\mathcal{M}' : \mathcal{H}_1 \rightarrow \mathcal{H}_3 \otimes \mathcal{H}_2$ (which depends on \mathcal{M}), and a simple global linear map with non-negative coefficients, $\mathcal{U} : (\mathcal{H}_3 \otimes \mathcal{H}_2) \otimes \mathcal{H}_2 \rightarrow \mathcal{H}_3$ (which is independent of \mathcal{M} , that is, universal, and given by $\mathcal{U}_{x_3 x_2 y_2}^{y_3} = \delta_{x_3}^{y_3} \delta_{x_2 y_2}$), such that $\mathcal{M} = \mathcal{U} \mathcal{M}'$.

Proof. If we adopt the convention that lower indices correspond to the input and upper indices to the output, we

can write \mathcal{M}' in terms of \mathcal{M} as $\mathcal{M}_{x_1}^{x_3 x_2} = \mathcal{M}_{x_1 x_2}^{x_3}$. The equality

$$\mathcal{M}_{x_1 y_2}^{y_3} = \sum_{x_2 x_3 y'_2} \mathcal{U}_{x_3 x_2 y'_2}^{y_3} (\mathcal{M}_{x_1}^{x_3 x_2} \delta_{y'_2}^{y_2}), \quad (4)$$

holds by definition. \square

Lemma 6. If the distribution $P_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is distillable, then for each $\lambda_0 \in [1/2, 1)$ there exists a distribution $Q_{ABE'} \in (\mathcal{B}_A \otimes \mathcal{H}_A) \otimes (\mathcal{B}_B \otimes \mathcal{H}_B) \otimes \mathcal{H}_{E'}$ such that

$$\Lambda[Q_{ABE'}] \leq \lambda_0, \quad (5)$$

$$\lambda[\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes P_{ABE}] > \lambda_0, \quad (6)$$

where \mathcal{U} is defined in Lemma 5. The size of $\mathcal{H}_{E'}$ is arbitrary.

Proof. Let n be the smallest integer such that there exist operations $\mathcal{M}_A : \mathcal{H}_A^{\otimes n} \rightarrow \mathcal{B}_A$ and $\mathcal{N}_B : \mathcal{H}_B^{\otimes n} \rightarrow \mathcal{B}_B$ such that $\lambda[\mathcal{M}_A \mathcal{N}_B P_{ABE}^{\otimes n}] > \lambda_0$ (following Definition 4). According to Lemma 5 there are maps $\mathcal{M}'_A, \mathcal{N}'_B$ such that $\mathcal{M}_A = \mathcal{U}_A \mathcal{M}'_A$, $\mathcal{N}_B = \mathcal{U}_B \mathcal{N}'_B$, and the distribution $Q_{ABE'} = \mathcal{M}'_A \mathcal{N}'_B P_{ABE}^{\otimes(n-1)}$ has alphabet $(\mathcal{B}_A \otimes \mathcal{H}_A) \otimes (\mathcal{B}_B \otimes \mathcal{H}_B) \otimes \mathcal{H}_{E'}$, as we want to show. Because Λ is defined through an optimization (Definition 3), we have

$$\Lambda[P_{ABE}^{\otimes(n-1)}] \geq \Lambda[\mathcal{M}'_A \mathcal{N}'_B P_{ABE}^{\otimes(n-1)}] = \Lambda[Q_{ABE'}]. \quad (7)$$

The definition of n implies that $\Lambda[P_{ABE}^{\otimes(n-1)}] \leq \lambda_0$, which together with (7), implies (5). Using the properties of the maps $\mathcal{U}, \mathcal{M}', \mathcal{N}'$ shown in Lemma 5, one can check that

$$\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes P_{ABE} = \mathcal{M}_A \mathcal{N}_B P_{ABE}^{\otimes n}. \quad (8)$$

Recall that the maps $\mathcal{M}_A, \mathcal{N}_B$ are the ones for which $\lambda[\mathcal{M}_A \mathcal{N}_B P_{ABE}^{\otimes n}] > \lambda_0$, which together with (8), implies (6). \square

In other words, what Lemma 6 tells is that if a distribution P_{ABE} is distillable, then it can activate the secrecy of another distribution Q_{ABE} . Here by activation we mean enhancement of the maximal extractable secret bit fraction $\Lambda[\cdot]$. The important point is that Alice's and Bob's alphabets in Q_{ABE} are bounded. Unfortunately, Lemma 6 does not tell anything about the size of Eve's alphabet in $Q_{ABE'}$, that is $\mathcal{H}_{E'}$, but this problem will later sort out itself.

IV. NON-DISTILLABILITY CRITERION

In order to certify that a given distribution $G_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is undistillable, it suffices to obtain a contradiction between the inequalities (5) and (6). However, the characterization of the set of distributions $Q_{ABE'} \in (\mathcal{B}_A \otimes \mathcal{H}_A) \otimes (\mathcal{B}_B \otimes \mathcal{H}_B) \otimes \mathcal{H}_{E'}$, where the

size of $\mathcal{H}_{E'}$ is arbitrary, satisfying $\lambda[\mathcal{M}_A \mathcal{N}_B Q_{ABE'}] \leq \lambda_0$ for any pair of maps $\mathcal{M}_A, \mathcal{N}_B$ is not available. Instead, we consider a larger (but simpler) set. For any given finite family of pairs of maps $\mathcal{F} = \{(\mathcal{M}_A^i, \mathcal{N}_B^i) : i = 1, \dots, M\}$, we consider the set of distributions which satisfy $\lambda[\mathcal{M}_A^i \mathcal{N}_B^i Q_{ABE'}] \leq \lambda_0$ for $i = 1, \dots, M$. In what follows we particularize to $\lambda_0 = 1/2$, although different criteria could be obtained for different values of λ_0 . Another big simplification is to write the inequalities (5) and (6) as “almost”-linear in the vector $Q_{ABE'}$. If we denote by e the variable of \mathcal{H}_E , and by e' the variable of $\mathcal{H}_{E'}$, we can write (5) and (6) as

$$2 \sum_{e', e} \min_{a \in \{0,1\}} \left\{ [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, a, e', e) \right\} - \frac{1}{2} \sum_{a, b, e', e} [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, b, e', e) > 0 \quad (9)$$

$$2 \sum_{e'} \min_{a \in \{0,1\}} \left\{ [\mathcal{M}_A^i \mathcal{N}_B^i Q_{ABE'}](a, a, e') \right\} - \frac{1}{2} \sum_{a, b, e'} [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABE'}](a, b, e') \leq 0, \quad (10)$$

for $i = 1, \dots, M$. This is obtained by using the explicit form of $\lambda[\cdot]$ given in (2), and setting $\lambda_0 = 1/2$.

Denote by d the dimension of \mathcal{H}_E . In (9) and (10) the summation over e runs over d values, while the summation over e' is unbounded (like the dimension of $\mathcal{H}_{E'}$). In what follows we transform the summation over e' into one over 2^{d+M} values. For each $e = 1, \dots, d$, define the function

$$r_e(e') = \begin{cases} 0 & \text{if } \sum_a (-1)^a [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, a, e', e) < 0 \\ 1 & \text{if } \sum_a (-1)^a [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, a, e', e) > 0 \end{cases}$$

for all e' . Analogously, for each $i = 1, \dots, M$ define the function

$$s_i(e') = \begin{cases} 0 & \text{if } \sum_a (-1)^a [\mathcal{M}_A^i \mathcal{N}_B^i Q_{ABE'}](a, a, e') < 0 \\ 1 & \text{if } \sum_a (-1)^a [\mathcal{M}_A^i \mathcal{N}_B^i Q_{ABE'}](a, a, e') > 0 \end{cases}$$

for all e' . Using these definitions we can write, for any value of e, i, e' ,

$$\min_{a \in \{0,1\}} \left\{ [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, a, e', e) \right\} = [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](r_e(e'), r_e(e'), e', e), \quad (11)$$

$$\min_{a \in \{0,1\}} \left\{ [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABE'}](a, a, e') \right\} = [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABE'}](s_i(e'), s_i(e'), e'), \quad (12)$$

which allows to get rid of the min-functions in (9) and (10). Let us define the new variable \mathbf{k} in the following way

$$\mathbf{k}(e') = (r_0(e'), r_1(e'), \dots, r_d(e'), s_1(e'), \dots, s_M(e')), \quad (13)$$

which has the natural distribution and correlations with A, B ,

$$Q_{ABK}(a, b, \mathbf{k}_0) = \sum_{e': \mathbf{k}(e') = \mathbf{k}_0} Q_{ABE'}(a, b, e') . \quad (14)$$

This allows to write the identities

$$\begin{aligned} & \sum_{e', e} \min_{a \in \{0,1\}} \left\{ [\mathcal{U}_A \mathcal{U}_B Q_{ABE'} \otimes G_{ABE}](a, a, e', e) \right\} \\ &= \sum_{\mathbf{k}, e} [\mathcal{U}_A \mathcal{U}_B Q_{ABK} \otimes G_{ABE}](k_e, k_e, \mathbf{k}, e) , \end{aligned} \quad (15)$$

$$\begin{aligned} & \sum_{e'} \min_{a \in \{0,1\}} \left\{ [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABE'}](a, a, e') \right\} \\ &= \sum_{\mathbf{k}} [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABK}](k_{d+i}, k_{d+i}, \mathbf{k}) , \end{aligned} \quad (16)$$

where we have used the fact that when $\{x_0 \leq x_1$ and $y_0 \leq y_1\}$ or $\{x_0 \geq x_1$ and $y_0 \geq y_1\}$ the equality

$$\min\{x_0, x_1\} + \min\{y_0, y_1\} = \min\{x_0 + y_0, x_1 + y_1\} \quad (17)$$

holds. After grouping the different values of e' as in (14), we only need to consider distributions Q_{ABK} where the variable \mathbf{k} runs over 2^{d+M} different values. However, the new (bounded in size) distribution Q_{ABK} must satisfy the constraints

$$\begin{aligned} & \sum_a (-1)^a [\mathcal{U}_A \mathcal{U}_B Q_{ABK} \otimes G_{ABE}](k_e \oplus a, k_e \oplus a, \mathbf{k}, e) < 0 , \\ & \sum_a (-1)^a [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABK}](k_{d+i} \oplus a, k_{d+i} \oplus a, \mathbf{k}) < 0 , \end{aligned}$$

for all e, i, \mathbf{k} .

Now everything is finite. Q_{ABK} is a vector from the space $(\dim \mathcal{H}_A \times \dim \mathcal{H}_B \times 2^{d+M+2})$ with non-negative components, that is $Q_{ABK}(a, b, \mathbf{k}) \geq 0$ for all a, b, \mathbf{k} . Hence, the set of allowed distributions Q_{ABK} is characterized by a finite set of linear inequalities. Then, maximizing the left-hand side of (9) is a linear programming

problem.

LINEAR PROGRAMMING: (18)

[If the maximum is zero then G_{ABE} is undistillable.]

$$\begin{aligned} & \max_{Q_{ABK}} \sum_{\mathbf{k}, e} \left(4[\mathcal{U}_A \mathcal{U}_B Q_{ABK} \otimes G_{ABE}](k_e, k_e, \mathbf{k}, e) - \right. \\ & \quad \left. - \sum_{a, b} [\mathcal{U}_A \mathcal{U}_B Q_{ABK} \otimes G_{ABE}](a, b, \mathbf{k}, e) \right) \end{aligned}$$

with constrains

$$\begin{aligned} & 4 \sum_{\mathbf{k}} [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABK}](k_{d+i}, k_{d+i}, \mathbf{k}) - \\ & \quad - \sum_{a, b, \mathbf{k}} [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABK}](a, b, \mathbf{k}) \leq 0 , \\ & \sum_a (-1)^a [\mathcal{U}_A \mathcal{U}_B Q_{ABK} \otimes G_{ABE}](k_e \oplus a, k_e \oplus a, \mathbf{k}, e) < 0 , \\ & \sum_a (-1)^a [\mathcal{M}_A^i \mathcal{M}_B^i Q_{ABK}](k_{d+i} \oplus a, k_{d+i} \oplus a, \mathbf{k}) < 0 , \\ & \sum_{a, b, \mathbf{k}} Q_{ABK}(a, b, \mathbf{k}) = 1 \\ & Q_{ABK}(a, b, \mathbf{k}) \geq 0 , \end{aligned}$$

for all $i = 1, \dots, M$, all $\mathbf{k} \in \{0, 1\}^{d+M}$, and all $a, b \in \{0, 1\}$ in the last inequality.

If the given distribution G_{ABE} has rational coefficients, the above linear programming can be solved by exact methods like the simplex algorithm [6]. Or by quasi-exact methods like the interior point algorithm [4], whose solution can always be certified exactly. The last method is faster, and hence can deal with larger values of M .

A key feature of this method is to choose a suitable family \mathcal{F} of pairs of maps. The larger the size of this family (M) the more constrains on the above maximization, and more chances to get the maximum equal to zero.

V. REMARKS

If the maximum of the linear programming (18) is zero then we know for sure that G_{ABE} is undistillable. But actually, we know something much stronger: G_{ABE} cannot activate any other non-distillable distribution. In other words, the correlations in G_{ABE} are completely useless.

Lemma 7. *Let the distribution G_{ABE} be such that the maximum of the linear programming (18) is zero. If P_{ABE} is a non-distillable distribution, then the tensor-product $P_{ABE} \otimes G_{ABE}$ is also non-distillable.*

Proof. By assumption, for any distribution Q_{ABE} such that $\Lambda[Q_{ABE}] \leq 1/2$ we have $\Lambda[Q_{ABE} \otimes G_{ABE}] \leq 1/2$. In particular, if we chose $Q_{ABE} = P_{ABE}^{\otimes n}$ we have

$\Lambda[P_{ABE}^{\otimes n} \otimes G_{ABE}] \leq 1/2$, for any n . But this also implies $\Lambda[(P_{ABE}^{\otimes n} \otimes G_{ABE}) \otimes G_{ABE}] \leq 1/2$, and proceeding by induction, we obtain $\Lambda[(P_{ABE} \otimes G_{ABE})^{\otimes n}] \leq 1/2$. \square

An interesting possibility is that for any distribution G_{ABE} with positive secrecy cost all linear programming problems (18) have a larger than zero maximum. This would imply that our criterion does not detect any non-distillable distribution, and hence it is useless. But this would also imply that any distribution G_{ABE} with positive secrecy cost (even though it may be non-distillable) can increase the quality of the secret bits distilled from a single copy of another distribution Q_{ABE} . Actually, an analog of the last statement is true in the quantum case [14, 15]. That is, all entangled states (of any number of parties) can increase the quality of the entanglement that can be distilled from a single copy of another state.

VI. CONCLUSION

In this paper, we have presented the first criterion which certifies that a given distribution G_{ABE} has no distillable key. In fact, this method consists on show-

ing that G_{ABE} does not improve the key content of *any* other distribution (i.e., it does not bring the maximally extractable secret bit fraction above $1/2$).

It is an open question whether all correlations with positive secrecy content can increase the secrecy of other correlations. This very interesting feature of secret correlations would invalidate the criterion presented here.

Finally, and perhaps most interestingly: does our technique have a quantum analogue, which could be used to prove the existence of entangled quantum states that do not contain secret key? This would present a complement to the work by Horodecki et al. [10], who show the existence of bound entangled states that do nevertheless contain secret key: perhaps there exists *completely bound entanglement* which neither contains distillable key nor enhances key content of other states.

Acknowledgments. LIM is supported by the spanish MEC (FIS2005-04627, FIS2007-60182, Consolider QOIT), and Caixa Manresa. AW is supported by the U.K. EPSRC (project "QIP IRC" and an Advanced Research Fellowship), and by a Royal Society Wolfson Merit Award.

-
- [1] A. Acín, J. I. Cirac, Ll. Masanes, "Multipartite Bound Information Exists and Can Be Activated", Phys. Rev. Lett., vol. 92, no. 10, 107903, 2004.
 - [2] R. Ahlswede, I. Csiszár, "Common Randomness in Information Theory and Cryptography — Part I: Secret Sharing", IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121-1132, 1993.
 - [3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A, vol. 54, no. 5, pp. 3824-3851, 1996.
 - [4] S. Boyd, L. Vandenberghe, "Convex Optimization", Cambridge University Press, Cambridge 2000.
 - [5] M. Christandl, R. Renner, S. Wolf, "A property of the intrinsic information", in: Proc. ISIT 2003, p. 258, 2003.
 - [6] V. Chvátal, *Linear Programming*, W. H. Freeman, New York, 1983.
 - [7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339-348, 1978.
 - [8] N. Gisin, S. Wolf, "Linking classical and quantum key agreement: is there 'bound information'?", in: Proc. Advances in Cryptology — CRYPTO 2000 (Santa Barbara, 20-24 August 2000), LNCS 1880, pp. 482-500, Springer Verlag, Berlin, 2000.
 - [9] M. Horodecki, P. Horodecki, R. Horodecki, "Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature?", Phys. Rev. Lett., vol. 80, no. 24, pp. 5239-5242, 1998.
 - [10] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, "Secure Key from Bound Entanglement", Phys. Rev. Lett., vol. 94, no. 16, 160502, 2005.
 - [11] M. Horodecki, P. Horodecki, R. Horodecki, "General teleportation channel, singlet fraction, and quasidistillation", Phys. Rev. A, vol. 60, pp. 1888-1898, 1999.
 - [12] N. S. Jones, Ll. Masanes, "Key Distillation and the Secret-Bit Fraction", IEEE Trans. Inf. Theory, Vol. 54, No. 2, pp 680-691 (2008).
 - [13] Ll. Masanes, A. Acín, "Multipartite Secret Correlations and Bound Information", e-print [cs.CR/0501008](#), 2005.
 - [14] Ll. Masanes, "All bipartite entangled states are useful for information processing", Phys. Rev. Lett. 96, 150501 (2006).
 - [15] Ll. Masanes, "Useful entanglement can be extracted from all nonseparable states", J. Math. Phys. 49, 022102 (2008).
 - [16] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information", IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733-742, 1993.
 - [17] U. Maurer, S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information", IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 499-514, 1999.
 - [18] A. Peres, "Separability Criterion for Density Matrices", Phys. Rev. Lett., vol. 77, no. 8, pp. 1413-1415, 1996.
 - [19] R. Renner, S. Wolf, "New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction", in: Proc. Advances in Cryptology — EUROCRYPT 2003, LNCS 2656, pp. 562-577, Springer Verlag, Berlin, 2003.
 - [20] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. Journal, vol. 28, no. 4, pp. 656-715, 1949.
 - [21] G. Vidal, J. I. Cirac, "Irreversibility in Asymptotic Manipulations of Entanglement", Phys. Rev. Lett., vol. 86, no. 25, pp. 5803-5806, 2001.
 - [22] A. Winter, "Secret, public, and quantum correlation cost

- of triples of random variables", ISIT 2005.
- [23] A. D. Wyner, "The Wire-Tap Channel", Bell Sys. Tech. J., vol. 54, pp. 1355-1387, 1975.